# REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188



| 1. REPORT DATE *(DD-MM-YYYY)* | 2. REPORT TYPE | 3. DATES COVERED (From – To) |
|---|---|---|
| 29 October 2003 | Final Technical Report | |

**4. TITLE AND SUBTITLE**

A Method For Allocating Financial Resources to Combat Terrorism: Optimizing the Reduction of Consequences

**5a. CONTRACT NUMBER**

**5b. GRANT NUMBER**

**5c. PROGRAM ELEMENT NUMBER**

**6. AUTHOR(S)**

Mackin, T.J., Henderson, Darrall, R., Jones, J.W.

**5d. PROJECT NUMBER**

**5e. TASK NUMBER**

**5f. WORK UNIT NUMBER**

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**

Department of Mathematical Sciences
United States Military Academy
West Point, NY 10996

**8. PERFORMING ORGANIZATOIN REPORT NUMBER**

**9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**

Military Operations Research Society
1703 North Beauregard Street, Suite 450
Alexandria, VA 22311

**10. SPONSOR/MONITOR'S ACRONYM(S)**

MORS

**11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

**12. DISTRIBUTION/AVAILABILITY STATEMENT**

Unclassified and Approved for Public Release; Distribution Unlimited

**13. SUPPLEMENTARY NOTES**

**14. ABSTRACT**

The National Strategy for Homeland Security established three strategic objectives: (1) Prevent terrorist attacks within the United States, (2) Reduce America's vulnerability to terrorism, and (3) Minimize the damage and recover from attacks that do occur. Objectives (1) and (3) essentially reprogram and re-prioritize activities within existing agencies such as the FBI, Customs, Cost Guard and FEMA, while objective 2 presents an entirely new examination of our Nation's infrastructure. Since the United States cannot counter all possible threats, the Department of Homeland Security is actively developing a risk-based management framework to prioritize vulnerabilities and to fund activities that most effectively reduce our nation's vulnerability to terrorist attack. This paper presents a mathematical framework for resource allocation to decrease America's vulnerability to terrorist attack. We introduce mathematical expressions that allow decision makers to allocate resources in a manner that maximizes the reduction in vulnerability to terrorist attack, subject to budget constraints. We introduce a delayed return function that captures the effect of long-term investments in risk-mitigation activities (such as R&D) that may not have short-term pay-off, but whose long-term contribution is substantial. We demonstrate the method using illustrative scenarios and a linear programming approach.



**15. SUBJECT TERMS** Combating Terrorism, Resource Allocation, Homeland Security, Reduction of Consequences

| 16. SECURITY CLASSIFCATION: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| Unclassified | | | UL | 17 | LTC Darrall Henderson |
| b. REPORT | b. ABSTRACT | c. THIS PAGE | | | 19b. TELEPHONE NUMBER (include area code) |
| Unclassified | Unclassified | Unclassified | | | (845) 938-4544 |

# *A METHOD FOR ALLOCATING FINANCIAL RESOURCES TO COMBAT TERRORISM: OPTIMIZING THE REDUCTION OF CONSEQUENCES*

T. J. Mackin,
Department of Mechanical and Industrial Engineering
The University of Illinois
1206 W. Green Street
Urbana, IL 61802
Voice: (217) 244-1016
Fax: (217) 333-1942

LTC Darrall Henderson
Department of Mathematical Sciences
United States Military Academy
West Point, NY 10996
Voice: (845) 938-4544
Fax: (845) 938-2409

J. W. Jones
J. William Jones Consulting Engineers, Inc.
16642 Island Circle #5
Huntington Beach, CA 92649
Voice: (714) 840-6723
Fax: (202) 429-9417

71st MORS Symposium
Working Group 16
13 June 2003

## Abstract

*The National Strategy for Homeland Security* established three strategic objectives: (1) Prevent terrorist attacks within the United States, (2) Reduce America's vulnerability to terrorism, and (3) Minimize the damage and recover from attacks that do occur. Objectives (1) and (3) essentially reprogram and re-prioritize activities within existing agencies such as the FBI, Customs, Cost Guard and FEMA, while objective 2 presents an entirely new examination of our Nation's infrastructure. Since the United States cannot counter all possible threats, the Department of Homeland Security is actively developing a risk-based management framework to

prioritize vulnerabilities and to fund activities that most effectively reduce our nation's vulnerability to terrorist attack. This paper presents a mathematical framework for resource allocation to decrease America's vulnerability to terrorist attack. We introduce mathematical expressions that allow decision makers to allocate resources in a manner that maximizes the reduction in vulnerability to terrorist attack, subject to budget constraints. We introduce a delayed return function that captures the effect of long-term investments in risk-mitigation activities (such as R&D) that may not have short-term pay-off, but whose long-term contribution is substantial. We demonstrate the method using illustrative scenarios and a linear programming approach.

**Introduction**

On September 11th 2001, war came to America. On January 24th, 2003, the Bush Administration established the Department of Homeland Security to respond to the threat of terrorism. This monumental reorganization of government, involving the combination of some 22 separate and distinct agencies, is under enormous pressure to remain one step ahead of our adversaries. Clearly, terrorists who would attack the United States have a wide variety of targets and methods from which to choose. Without a full-scale military mobilization, and in the spirit of maintaining a sense of normalcy in daily life, it becomes exceedingly difficult to defend an infrastructure as vast as that in the United States: especially since freedom of movement and personal liberty are at the very core of American society.

The problem of securing our infrastructure is enormous. Our nation has over 168,000 public water systems; 300,000 oil and natural gas production sites, 177,000 miles of oil pipeline; 1.3 million miles of natural gas pipelines; 3.95 million miles of public roads; 582,976 bridges; 1.2 million miles of rail and over 18,760 general aviation airports[1]. The United States cannot afford to monitor and protect such a vast and distributed infrastructure. Instead, we must prioritize and invest in a manner that provides the greatest possible protection for the population. This paper presents a formalized approach to allocating financial resources to reduce America's vulnerability to terrorist attacks. The method is based on risk management methodology, which

is widely used in a broad range of industries, including: the insurance industry, industrial plant maintenance and inspection programs, and risk-based decision analysis. The proposed approach is applicable to any attack scenario that can be quantified by a probability of occurrence and an estimated cost of damage.

In order to apply an optimization scheme, it is important to first establish a generic approach to ranking terrorist threats. Our proposed approach, based on risk management methodology, is graphically illustrated in Figure 1, where the probability of success, *PS*, of a terrorist attack is plotted against the dollar cost-of-consequences (*DCC*) of that attack. Theoretically, every conceivable threat can be located on this graph through the ordered pair (*DCC*, *PS*). The goal of counter terrorism is to reduce the probability of success to an agreed upon acceptable level. That is, resources would be allocated so that all conceivable threats lie below some agreed upon probability of success, or to the left of some line of constant weighted risk consequence. Clearly, resources would not be allocated uniformly across all conceivable threats, but would be allocated to greatest benefit. Some threats are so unlikely that no resources are required. Others would require immediate attention. As such, the first step in designing an investment strategy begins with establishing a uniform approach to quantifying each threat.

Each threat scenario can be evaluated using *Fault Tree Analysis* (See Ebeling, 1997) to obtain a probability of success, wherein the scenario is decomposed into independent steps, each of which must be performed successfully for the overall attack to be successful. The overall *Probability of Success* (***PS***) of the scenario is the product of the probabilities of success for each sub-step in the scenario. The probability of success may depend on many variables, all of which factor into the overall success of the attack.

A graph, such as Figure 1, serves as a master curve for plotting, ranking, and comparing all possible terrorist threats. The graph is populated using threat assessments for each attack scenario to generate a *Probability of Success* and a *Dollar Cost of Consequences*. The scale for the y-axis runs from a probability of 0.0 (no chance of success) to 1.0 (100% probability of success). We identify the set of all such points as the vulnerability manifold. We use this notion in the next section where we formalize a proposed investment model. Using this method, any

threat can be evaluated and plotted on the same graph. The value of the scheme is obvious. It can be used to compare any kind of threat and determine which is the most severe in terms of cost to the United States. Loss of life and permanent injury to Americans is key to evaluating any threat. It is assumed that any casualties would also be assigned a *Dollar Cost of Consequence*. This is not intended to represent the value of a life, but is included only to provide a basis of comparison of different events.

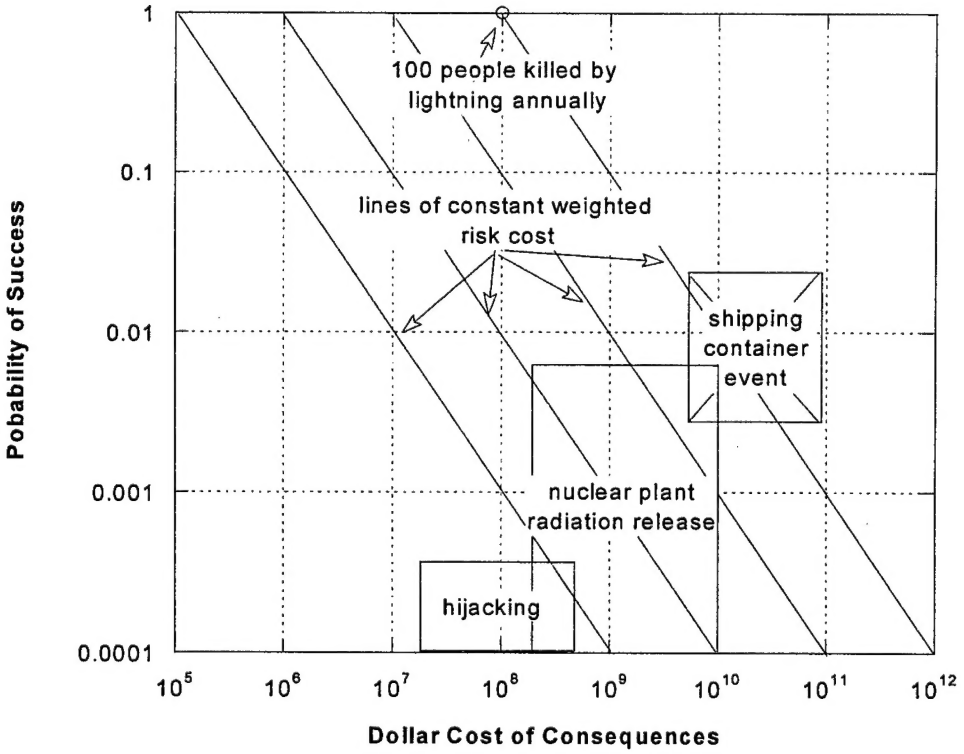



**Figure 1.** Vulnerability plot for organizing terrorist threats. Probability of success is plotted against cost of consequences. The product of each is the weighted cost of consequences. Lines of constant weighted cost have been placed into the figure. Several illustrative threat scenarios have been overlain on the graph.

The product of *Dollar Cost of Consequences* and *Probability of Success* is defined as the *Weighted Risk Cost,* $R_i$. The *Weighted Risk Cost* is a measure of the value of the assets that are at-risk. Once a collection of various terrorist threats are plotted, each threat can be ranked

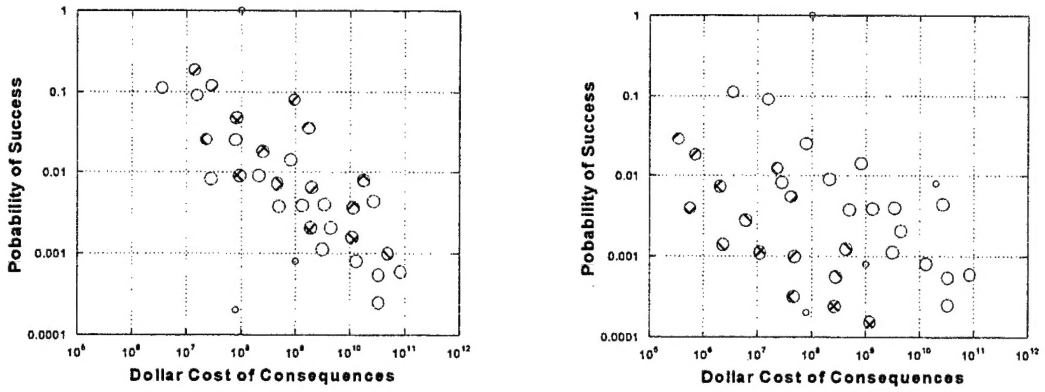
according to the *Weighted Risk Cost*. The graph can then be divided into zones to develop an investment strategy to reduce every threat to a specified acceptable level, or, as is shown in the next section, one can use a global optimization approach. In any case, threat mitigation strategies should be developed to extract the greatest benefit from the investment.

**Allocating Resources**

As with any investment strategy, the investment to combat terrorism involves a finite amount of money. The question then becomes, what is the most effective allocation of these scarce resources? Not only must the money be distributed to a finite number of vulnerabilities, the money must also be parsed among those vulnerabilities. In order to formalize this approach, consider the identification of N-total vulnerabilities. Furthermore, we presume that the available resources may not be sufficient to redress all of the identified vulnerabilities. As such, we are faced with the problem of how best to allocate the available resources.

In the most general approach, our resources may only be sufficient to address some subset, $\boldsymbol{k}$, of the $N$-vulnerabilities. Each of these represents an investment in a *Threat-Mitigation Program* (*TMP*), where $k$ is less than or equal to $N$. The task of the optimization effort is to choose *k-TMP*s, as well as the amount of money invested in each of those *k-TMPs*, to maximize the *Reduction in Vulnerability* (*RV*). It is worth noting that one must also choose subsets based on intelligence agency input. That is, identify the most likely targets.

Figure 2 schematically illustrates the effect of investing in threat mitigation programs, where we show how a hypothetical investment strategy that addresses a subset of the total number of threats and shifts the corresponding vulnerability manifold down. In this representation we ignore the uncertainties in probabilities of success, however, they do exist.




(a) (b)

**Figure 2.** A subset of the total vulnerabilities have been outlined in red in (a). These vulnerabilities are reduced (b) by a threat mitigation program.

**The key question that faces decision makers is:** *which Threat-Mitigation Programs should be funded, and how should the funds be parsed among those programs?*

To properly answer this question, we must construct a function that, in the present case, captures the reduction in total vulnerability brought about by investing the available funds within and across the space of identified vulnerabilities. Once this function is constructed, the investment decision amounts to an optimization problem, whereby the investors choose the funding allocation scheme that maximizes the *Reduction in Vulnerability*. We improve the analysis by using delayed-return investment functions that incorporate tunable delay times into the return-functions.

Delayed-investment strategies are those that depend on new technology generated by Research and Development. These strategies would do nothing in the short-term to reduce vulnerabilities, but may, in the long-term, provide the optimum overall *Reduction in Vulnerability*. This is a key point that must be emphasized: *the return on investment depends on the time frame over which one measures that return*. As a result, it is important to note that the optimum investment portfolio may be very different for a long-term strategy than that for a short-term strategy.

Additionally, one must consider the possibility of a dynamic strategy whereby the investment portfolio is restructured at the maturation of each R&D program.

Typically, the resources allocated to the proposed investment problem are constrained to a specific total amount: designated as the *Total Allocated Investment*, $B_T$. This investment is distributed among $k$-chosen *Threat-Mitigation Programs*, each of which costs an amount $C_j$. Regardless of the allocation scheme selected, the sum of the individual *Threat-Mitigation Program* costs must equal the *Total Allocated Investment*. That is:

$$B_T = \sum_{i=1}^{k} C_i \tag{1}$$

Where $B_T$ is the total amount invested in year $T$

$C_i$ is the amount invested in a *Threat-Mitigation Program toward vulnerability i*

$k$ is the total number of *Threat-Mitigation Programs*.

Note that we have not decided which *Threat-Mitigation Programs* to fund, nor have we decided how many *Threat-Mitigation Programs* to fund. Both of these decisions are intended as outputs from the optimization problem.

In order to judge the effect of investment on the *Reduction in Vulnerability*, we need to construct a function that adequately represents that effect. Hence, we use the framework adopted earlier to plot the probability of success against the Cost-of-Consequences for each vulnerability. A reduction in the vulnerability of a particular asset decreases the probability of success. The probability of success as a function of investment is represented as follows:

$$PS_i = PO_i \cdot e^{-C_i / D_i} \tag{2}$$

Where $PS_i$ is the probability of success of vulnerability $i$ at an investment of $C_i$

$D_i$ is the damping factor for vulnerablity $i$

$PO_i$ is the un-mitigated probability of success of vulnerability *i*.

Note that $PS_i \leq PO_i$ and that a $C_i \geq 0$ will reduce $PS_i$

The exponential function in Equation 2 is used to represent a diminishing returns investment that decreases the asset vulnerability hence, reduces the probability of a successful attack. The investment is scaled using a damping ratio that sets the rate of diminishing returns. Note that this function has a derivative that is everywhere negative, and is concave up.

A plot of Equation 2 for a range of damping factors is shown in Figure 3. The variety of return functions based on different damping factors illustrates the role of the damping factor. The nature of the reduction in threat will determine the amount of money spent: rapidly decaying functions require less investment than more slowly decaying functions. In either case, the functional form plays a vital role in allocating the existing resources.

Given the exponential decay in the probability of success with investment, it is easy to compute the *Reduction in the Weighted Risk Cost* of Consequences as the difference between the unmitigated cost and mitigated costs, as follows:

$$R_i = (PO_i \cdot DCC_i) - (PO_i \cdot DCC_i \cdot e^{-C_i / D_i}) \tag{3}$$

$$R_i = PO_i \cdot DCC_i (1 - e^{-C_i / D_i}) \tag{4}$$

Where $R_i$ is the *Reduction in the Weighted Risk Cost* for vulnerability *i*. A sample plot of this function is shown in Figure 4, illustrating the effect of investment for an exponential function.

The total *Reduction in the Weighted Risk Cost* of consequences, then, is the sum over the *k-Threat-Mitigation Programs*:

$$\textit{Total Reduction in the Weighted Risk Cost} = \sum_{i=1}^{k} PO_i \cdot DCC_i \left(1 - e^{-C_i / D_i}\right) \qquad (5)$$

This is the function that must be maximized in order to choose the best investment strategy.

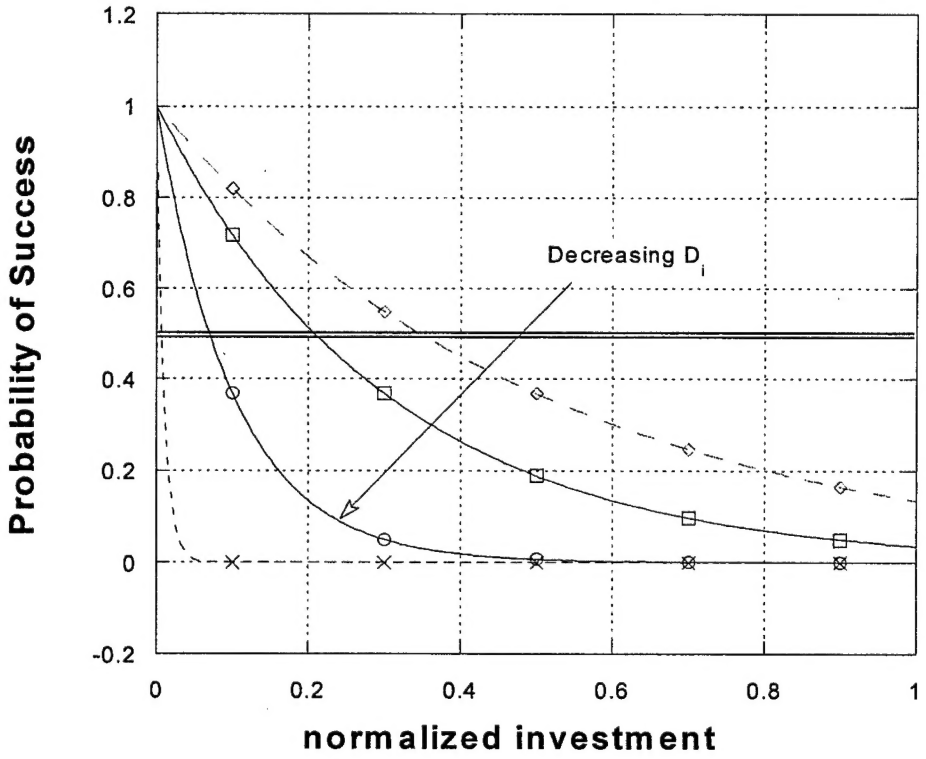



**Figure 3.** Sample plot of an exponential decay in probability of success as a function of dollars invested. This illustrates that decay rates can vary depending on the damping factor. A horizontal line is drawn at the 50% probability level. This is a convenient comparison, since it can be used to compare the various curves, that is, the cost required to decrease the probability of success by 50%.

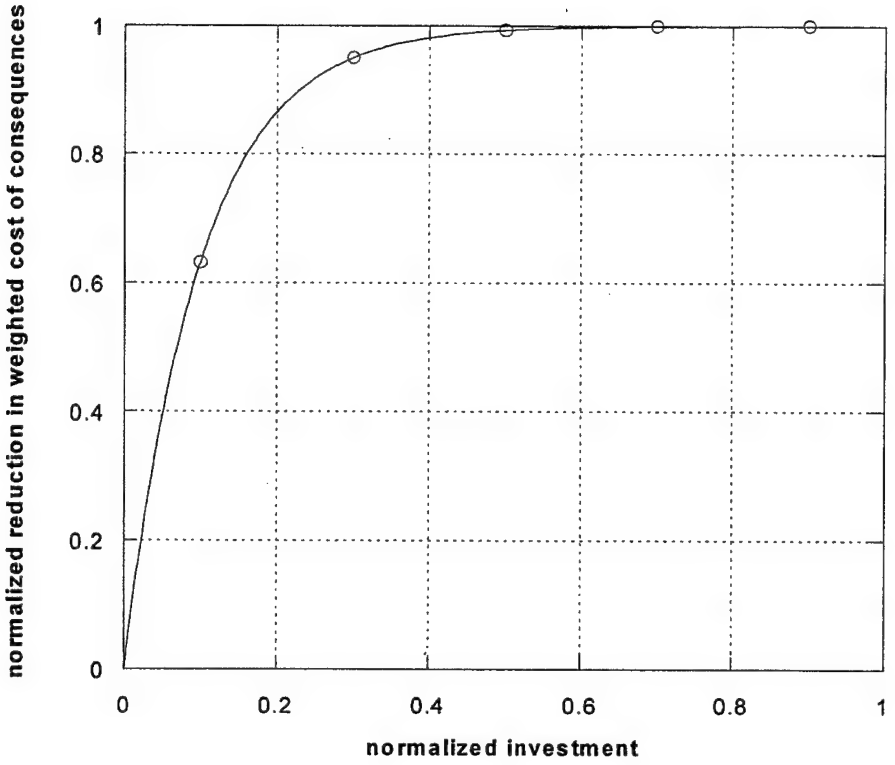



**Figure 4.** Sample plot of the reduction in weighted cost of consequences for a single threat scenario. This plot shows that the greatest reductions come from the early investments, and shows that beyond a reduction of 90% substantially increasing amounts of investment are required for only marginal returns.

This function does not take into account any time delay factors. As such, the function does not account for any dynamic delay effects resulting from investments in R&D activities. Hence, the function in Equation 5 is most applicable to operational aspects, and not to R&D investments. To account for time-delays associated with emerging technologies, we introduce a heavy-side function, defined as follows:

$$H_i = \begin{cases} 0 \text{ if } T < t_i \\ 1 \text{ if } T \geq t_i \end{cases} \tag{6}$$

This function is used to 'turn on' the diminishing returns probability of success function at a delayed time specified by $t_i$. The delay time, $t_i$ represents the time when a return on investment for *Threat Reduction Program i* is expected. A time-delayed *Reduction in the Weighted Risk Cost* of Consequences function is represented by:

$$R_i = PO_i \cdot DCC_i (1 - H_i \cdot e^{-C_i / D_i}) \tag{7}$$

This modified function will not reduce the weighted cost of consequences for time frames less than $t_i$, therefore, it does not show an immediate return. This is an important issue to consider, since there will be certain vulnerabilities that are simply not amenable to mitigation using current technology. That is, certain probabilities *simply can not* be reduced without an R&D effort, so expenditures in R&D are crucial to mitigating certain threat categories. A sample plot of Equation 7 is shown in Figure 5, illustrating that no reduction in probability of success occurs until the heavyside function turns on. It is worth noting that we are swapping delay times and investment dollars. We do this because there will be a relationship between the amount invested and the time for returns. This mapping between time and dollars varies for each *Threat Reduction Program*. However, it is sufficient to note that there is a relationship between investment and time, and that some mitigation efforts may require considerable investment before yielding any returns. The total reduction in weighted cost of consequences is represented by:

$$\textit{Total Reduction in the Weighted Risk Cost} = \sum_{i=1}^{k} PO_i \cdot DCC_i (1 - H_i \cdot e^{-C_i / D_i}) \tag{8}$$

We acknowledge that the key to using this approach successfully lies in accurate determinations of the probability of success, $PS_i$, the *Dollar Cost of Consequence* of an attack, $DCC_i$, the scale factor that determines the damping of returns for an investment, $D_i$, and the delay time for deliverables of new technology, $t_i$. These are crucial inputs that remove subjectivity from the problem and parameters that require a great deal of attention in order to reducing the subjectivity of the analysis. Failure to reduce the subjectivity of these parameters results in a resource

allocation strategy of greasing squeaky wheels; where the most vocal advocate reaps the largest rewards. However, certain aspects of this problem will always retain a degree of subjectivity, for instance, probability of success, and cost of consequences when these consequences include loss of life.

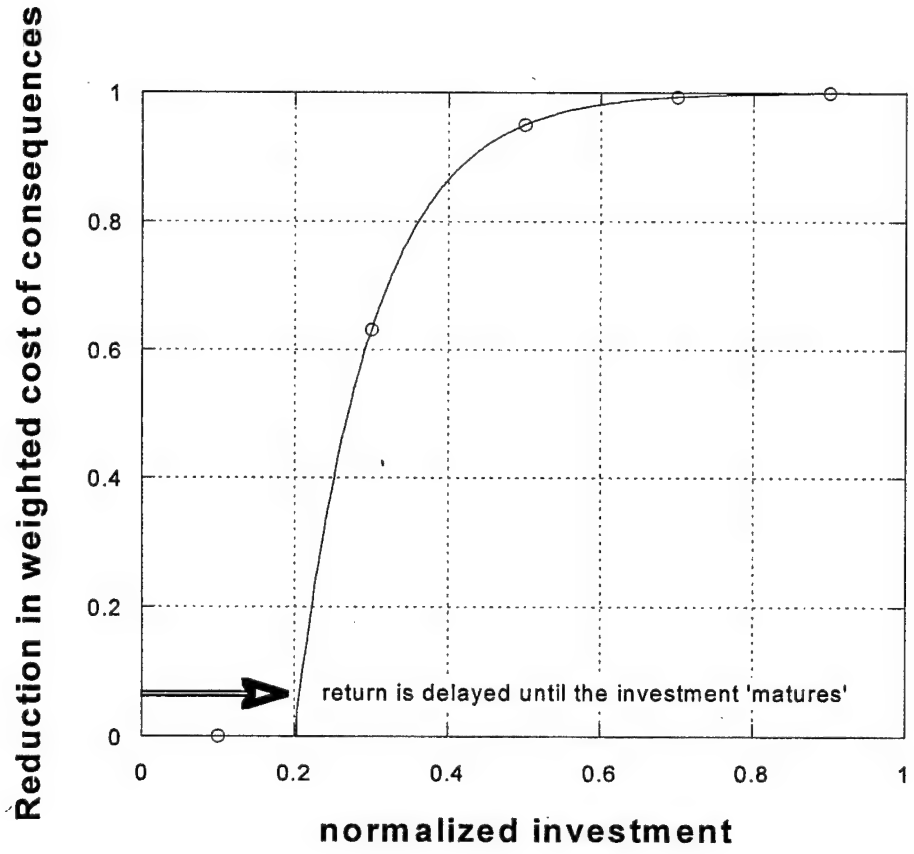



**Figure 5.** Sample plot showing the effect of a delayed return on investment. In this case, the reduction in probability of success is not seen until the R&D investment has matured.

**Computational Experiments**

To answer the original question: *which Threat-Mitigation Programs should be funded, and how should the funds be parsed among those programs?* Equation (8) can be used to model the *Total Reduction in the Weighted Risk Cost* using a simple integer program designed to Maximize the *Total Reduction in the Weighted Risk Cost* without exceeding the budget, $B_T$, in year $T$.

$$\textit{Maximize} \qquad \sum_{i=1}^{k} PO_i \cdot DCC_i (1 - H_i \cdot e^{-C_i / D_i})$$

$$\text{Subject to: } I_T = \sum_{i=1}^{k} C_i \le B_T$$

$$D_i > 0, C_i \ge 0, DCC_i \ge 0, t_i \ge 0, T \ge 0, B_T \ge 0, I_T \ge 0, PO_i \le 1,$$

$$\text{and } H_i = \begin{cases} 0 \text{ if } T < t_i \\ 1 \text{ if } T \ge t_i \end{cases}$$

This integer program can be modeled and optimized using any number of mathematical programming or spreadsheet software packages. To demonstrate the utility of this approach, a sample problem consisting of twelve potential threats was modeled using Microsoft Excel and solved using the basic solver tool provided with Excel. Note that the solver provided with Excel has limited capacity, hence, larger models may require an enhanced solver available from Frontline Systems. The objective of the computational experiment is to develop an *Optimal Threat Mitigation Scenario* (i.e., identify a portfolio of *Threat Mitigation Programs* to be funded) that maximizes the *Reduction in the Weighted Risk Cost* without breaking annual budgetary constraints using an off the shelf spreadsheet software program.

Twelve notional threats were identified with corresponding *Dollar Cost of Consequences*, $DCC_i$, *Probability of Occurrence*, $PO_i$, and the amount invested in each *Threat Mitigation Program*, $C_i$ over a six year planning horizon, FY03 through FY08 (Table I). Technology delays and the damping factor, $D_i$, associated with each of the threat reduction programs were accounted for in a separate section of the spreadsheet (Table II) and referred to when calculating the overall *Reduction in Weighted Risk Cost* for each *Threat Mitigation Program* over the six year time horizon (Table III). Each funding year has a budget cap that cannot be exceeded by the sum of the cost of *Threat Mitigation Programs* funded in that year (the Budgeted row in Table III).

**Table I**

Cost of threat mitigation programs, probability of occurrence and dollar cost of consequences for each threat

| Threat # | FY03 | FY04 | FY05 | FY06 | FY07 | FY08 | $PO_i$ | $DCC_i$ |
|---|---|---|---|---|---|---|---|---|
| 1 | $100,000 | $101,000 | $105,000 | $109,295 | $112,418 | $116,781 | 0.90 | $800,000 |
| 2 | $88,000 | $75,000 | $74,902 | $74,345 | $75,981 | $77,922 | 0.25 | $700,000 |
| 3 | $54,807 | $66,000 | $57,402 | $55,647 | $57,087 | $58,610 | 0.90 | $654,000 |
| 4 | $6,500 | $23,000 | $30,000 | $10,948 | $11,239 | $11,515 | 0.23 | $630,000 |
| 5 | $22,000 | $23,000 | $15,000 | $13,887 | $14,227 | $14,582 | 0.50 | $2,200,000 |
| 6 | $54,691 | $54,514 | $56,580 | $56,914 | $58,282 | $59,686 | 0.45 | $540,000 |
| 7 | $8,989 | $7,408 | $6,565 | $6,701 | $7,182 | $10,740 | 0.33 | $370,000 |
| 8 | $44,000 | $40,000 | $30,000 | $26,652 | $25,888 | $22,993 | 0.20 | $220,000 |
| 9 | $18,252 | $19,011 | $19,233 | $20,100 | $20,684 | $21,288 | 0.85 | $290,000 |
| 10 | $22,000 | $35,000 | $40,000 | $18,682 | $19,234 | $19,804 | 0.44 | $330,000 |
| 11 | $19,000 | $20,000 | $18,056 | $18,645 | $19,196 | $19,764 | 0.22 | $220,000 |
| 12 | $23,000 | $24,000 | $20,000 | $18,738 | $19,291 | $19,861 | 0.20 | $340,000 |
| Total | $461,239 | $487,933 | $472,738 | $430,554 | $440,709 | $453,546 | | |

**Table II**

Technology delay for each threat-mitigation program

| Threat # | FY03 | FY04 | FY05 | FY06 | FY07 | FY08 |
|---|---|---|---|---|---|---|
| 1 | Yes | Yes | Yes | No | No | No |
| 2 | No | No | No | No | No | No |
| 3 | No | No | No | No | No | No |
| 4 | Yes | Yes | Yes | No | No | No |
| 5 | No | No | No | No | No | No |
| 6 | No | No | No | No | No | No |
| 7 | No | No | No | No | No | No |
| 8 | Yes | Yes | No | No | No | No |
| 9 | No | No | No | No | No | No |
| 10 | No | No | No | No | No | No |
| 11 | No | No | No | No | No | No |
| 12 | No | No | No | No | No | No |

The Fund/No Fund column in Table III determines whether or not a particular *Threat Mitigation Program* will be included in *Optimal Threat Mitigation Scenario* (i.e., portfolio of *Threat Mitigation Programs* used to address specific threats). The Fund/No Fund column consists of zeros and ones: one meaning that the *Threat Mitigation Program* is funded and zero implying that the *Threat Mitigation Program* is not funded. The columns labeled FY03 through FY08 contain the *Reduction in the Weighted Risk Cost*, $R_i$ base on Equation 4, for each *Threat Mitigation Program* over the funding horizon. Note that the $R_i$ values for each *Threat Mitigation Program* may differ over the time horizon due to changes in the annual cost of the *Threat Mitigation Program* for the given year (see Tables I and III). Additionally, if there is a time delay in the effectiveness of the technology, the value in the *Reduction in Weighted Risk Cost* cell will be zero, implying that even though funds are spent on a *Threat Mitigation Program*, the

program has no value added in the given year (i.e., the heavy side function in Equation 6 dominates the value).

**Table III**

Total reduction in cost of consequences with all programs funded

| Threat # | Fund/No Fund | Delay | FY03 | FY04 | FY05 | FY06 | FY07 | FY08 | Reduction | Product |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | Yes | 0 | 0 | 0 | 358741 | 358741 | 358741 | 1076222 | 1076222 |
| 2 | 1 | No | 87194 | 87194 | 87194 | 87194 | 87194 | 87194 | 523163 | 523163 |
| 3 | 1 | No | 293271 | 293271 | 293271 | 293271 | 293271 | 293271 | 1759623 | 1759623 |
| 4 | 1 | Yes | 0 | 0 | 0 | 72197 | 72197 | 72197 | 216590 | 216590 |
| 5 | 1 | No | 548076 | 548076 | 548076 | 548076 | 548076 | 548076 | 3288456 | 3288456 |
| 6 | 1 | No | 121075 | 121075 | 121075 | 121075 | 121075 | 121075 | 726450 | 726450 |
| 7 | 1 | No | 60836 | 60836 | 60836 | 60836 | 60836 | 60836 | 365019 | 365019 |
| 8 | 1 | Yes | 0 | 0 | 21923 | 21923 | 21923 | 21923 | 87692 | 87692 |
| 9 | 1 | No | 122819 | 122819 | 122819 | 122819 | 122819 | 122819 | 736913 | 736913 |
| 10 | 1 | No | 72346 | 72346 | 72346 | 72346 | 72346 | 72346 | 434076 | 434076 |
| 11 | 1 | No | 24115 | 24115 | 24115 | 24115 | 24115 | 24115 | 144692 | 144692 |
| 12 | 1 | No | 33881 | 33881 | 33881 | 33881 | 33881 | 33881 | 203286 | 203286 |
| | | | | | | | Total Reduction in Cost of Conseqences = | | | 9562183 |
| | | | | | | | | | | |
| | | Budgeted | $400,000 | $410,000 | $410,000 | $420,000 | $440,000 | $445,000 | $2,525,000 | |
| | | | <= | <= | <= | <= | <= | <= | <= | |
| | | Funded | $461,239 | $487,933 | $472,738 | $430,554 | $440,709 | $453,546 | $2,746,719 | |

The column marked Reduction in Table III is the sum of the *Reduction in the Weighted Risk Cost* for each *Threat Mitigation Program* over the funding horizon. If the *Threat Mitigation Program* is funded, a one is placed in the Fund/No Fund column corresponding to the *Threat Mitigation Program* and the *Total Reduction in the Weighted Risk Cost* is reflected in the Product column in Table III. Additionally the annual costs associated with each *Threat Mitigation Program* are summed and reflected in the Funded row (i.e., the total annual cost of all funded *Threat Mitigation Programs*). Note that the amount in the Funded row in Table III exceeds the amount Budgeted for each year in the funding horizon, a strategy that violates one of the constraints in the integer program. As such, Table III reflects a *Threat Mitigation Scenario* that funds all twelve *Threat Mitigation Programs*. Although desirable, this *Threat Mitigation Scenario* is infeasible since it violates one of the constraints in the integer program. Using the solver tool in Microsoft Excel, an *Optimal Threat Mitigation Scenario* is proposed in Table IV. Note that three of the *Threat Mitigation Programs* are not funded (numbers 8, 11, and 12), but none of the budget constraints are violated. Note that the unfunded *Threat Mitigation Programs* result in no value added to the overall *Total Reduction in the Weighted Risk Cost*. This same technique can be extended to a more realistic problem consisting of more threats and a longer funding horizon.

**Table IV**

Total reduction in cost of consequences with optimal program funding scheme

| Threat # | Fund/No Fund | Delay | FY03 | FY04 | FY05 | FY06 | FY07 | FY08 | Reduction | Product |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | Yes | 0 | 0 | 0 | 358741 | 358741 | 358741 | 1076222 | 1076222 |
| 2 | 1 | No | 87194 | 87194 | 87194 | 87194 | 87194 | 87194 | 523163 | 523163 |
| 3 | 1 | No | 293271 | 293271 | 293271 | 293271 | 293271 | 293271 | 1759623 | 1759623 |
| 4 | 1 | Yes | 0 | 0 | 0 | 72197 | 72197 | 72197 | 216590 | 216590 |
| 5 | 1 | No | 548076 | 548076 | 548076 | 548076 | 548076 | 548076 | 3288456 | 3288456 |
| 6 | 1 | No | 121075 | 121075 | 121075 | 121075 | 121075 | 121075 | 726450 | 726450 |
| 7 | 1 | No | 60836 | 60836 | 60836 | 60836 | 60836 | 60836 | 365019 | 365019 |
| 8 | 0 | Yes | 0 | 0 | 21923 | 21923 | 21923 | 21923 | 87692 | 0 |
| 9 | 1 | No | 122819 | 122819 | 122819 | 122819 | 122819 | 122819 | 736913 | 736913 |
| 10 | 1 | No | 72346 | 72346 | 72346 | 72346 | 72346 | 72346 | 434076 | 434076 |
| 11 | 0 | No | 24115 | 24115 | 24115 | 24115 | 24115 | 24115 | 144692 | 0 |
| 12 | 0 | No | 33881 | 33881 | 33881 | 33881 | 33881 | 33881 | 203286 | 0 |
| | | | | | | | Total Reduction in Cost of Conseqences = | | | 9126513 |
| | | | | | | | | | | |
| | | Budgeted | $400,000 | $410,000 | $410,000 | $420,000 | $440,000 | $445,000 | $2,525,000 | |
| | | | <= | <= | <= | <= | <= | <= | <= | |
| | | Funded | $375,239 | $403,933 | $404,682 | $366,519 | $376,334 | $390,928 | $2,317,635 | |

In summary (see Table IV), the objective of the spreadsheet model is to maximize the *Total Reduction in the Cost of Consequences* found at the bottom of the Product column while keeping the values in the Funded row less than the values in the Budgeted row for each year in the funding horizon. This is accomplished by changing values in the Fund/No Fund column from zero to one until an optimal solution is reached. This integer programming solution is accomplished using the solver tool supplied with Microsoft Excel. This simple spreadsheet model answers the original question: *which Threat-Mitigation Programs should be funded, and how should the funds be parsed among those programs* by Maximizing the *Total Reduction in the Weighted Risk Cost* without exceeding the budget, $B_T$, in year $T$.

Although optimal and feasible from a mathematical point of view, this solution may not be acceptable from a practical or political point of view. However, it does provide a means of comparing potential solutions and is a good starting point for decision makers as they strive to define an acceptable *Threat Mitigation Program*.

## Conclusions

We developed a mathematical model to capture the return on investment for threat mitigation programs in the war on terror. This model includes a diminishing returns exponential investment function with a tunable damping factor, a weighted cost of consequences function, and a time delayed return on investment switch. The model was then cast into the framework of an

optimization problem by maximizing the decrease in the weighted cost of consequences function. We showed that this model can be optimized using a linear program operating in the EXCEL software program, providing a simple, user-friendly tool for decision making and budgeting in the war on terror.

## Endnotes

[1] As outlined in the National Strategy for The Physical Protection of Critical Infrastructures and Key Assets, February 2003.

## References

Ebeling, C.E. 1997. An Introduction to Reliability and Maintainability Engineering. McGraw-Hill, 172-178.

## Descriptors

Homeland defense
Homeland security
Combating terrorism
Threat mitigation
Allocating resources
Reduction of consequences
Reduction in vulnerability